35 U.S.C. §103(a) MENEZES REJECTION

Claims 1-22 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes, et al, (Handbook of Applied Cryptography). This rejection, in so far as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

Applicant respectfully submits that the present invention, as recited in independent claims 1 and 12, recites initiating two challenges, each of which is answered by a challenge response. In the arrangement recited in independent claims 1 and 12, the first challenge is a random number and the second challenge is a count value. By utilizing a count value as the second challenge, the protocol defined by the present invention is a secure protocol.

In formulating the rejection under 35 U.S.C. §103(a), the Examiner primarily relies on page 402 of Menezes. Applicant respectfully submits that the arrangement described on page 402 of Menezes utilizes two (2) random numbers as the first and second challenges. The use of two (2) random numbers resulted in insecure protocol, which is undesirable.

Accordingly, applicant has improved upon the Menezes two (2) random number challenge arrangement by modifying the second challenge to be a count value, in order to provide a secure protocol.[1] Menezes does not identify

[1] Applicant has also provided additional portions of Menezes, which also confirm that Menezes fails to teach or suggest the dual challenge arrangement of independent claims 1 and 12, wherein the first challenge is random number and the second challenge is a count value.

protocol security as a problem to be solved. Further, even if Menezes did identify such a problem, Menezes does not teach or suggest to one of ordinary skill in the art that replacement of the second random number challenge with a count value challenge would provide a secure protocol. Accordingly, applicant respectfully submits that Menezes does not render obvious independent claims 1 or 12 of the present application alone.

On page 6 of the outstanding Office Action, the Examiner refers to U.S. Patent 5,515,439 to Bantz for allegedly teaching offsetting a counter value to an arbitrary initial value and an authentication protocol to make eavesdropping and replay attacks from intruders more difficult.

Initially, if the Examiner wishes to rely on the teachings of Bantz et al in the present rejection, applicant requests the Examiner to reformulate the rejection as a 35 U.S.C. §103(a) combination rejection in view of Menezes and Bantz, and to supply the requisite motivation for combining these two references. Assuming that the Examiner does choose to reply on the combination of Menezes and Bantz, applicant still respectfully submits that although the abstract of Bantz teaches protection against potential eavesdroppers and intruders by combining cryptographically the elements of an exchange certificate, neither Bantz alone nor the combination of Bantz and Menezes teach or suggest the use of two (2) challenges, wherein the first challenge is a random number and the second challenge is a count value.

Accordingly, applicant respectfully submits that independent claims 1 and 12 are allowable for at least this additional reason.

Applicant respectfully submits that dependent claims 2-11 and 13-22 are patentable by virtue of their dependency on allowable independent claims 1 or 12 for at least the reasons set forth above.

CONCLUSION

In view of the above amendments and remarks, reconsideration of the rejection and allowance of claims 1-22 is respectfully requested.

In the event that there are any outstanding matters remaining in the present application, the Examiner is invited to contact John A. Castellano at (703) 205-8000 in the Washington, D.C. area, to discuss this application.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant respectfully petitions for a two (2) month extension of time for filing a reply in connection with the present application, and the required fee of $390.00 is attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 12-2325 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH STEWART KOLASCH & BIRCH, LLP

By:_____
John A. Castellano
Registration No. 35,094

JAC:cb

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

Enclosures: Pages 497, 499, 535 and 707 of Menezes